

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

| | | |
|---------------------------------|---|---|
| UNITED STATES OF AMERICA | : | |
| | : | |
| v. | : | CRIMINAL NO. 05-193-02 & 05-193-13 |
| | : | |
| AKHIL BANSAL | : | |
| | : | |
| MATTHEW MELAO | : | |

**GOVERNMENT’S OPPOSITION TO DEFENDANT AKHIL BANSAL’S *PRO SE*
MOTIONS TO SUPPRESS EVIDENCE FROM ELECTRONIC SURVEILLANCE
(DOCKET NOS. 308 & 309 & 310) AND DEFENDANT MATTHEW MELAO’S *PRO SE*
MOTION TO SUPPRESS ELECTRONIC EVIDENCE (DOCKET NO. 280)**

The United States of America, by and through its attorneys, Patrick L. Meehan, United States Attorney for the Eastern District of Pennsylvania, Frank Costello and Bea Witzleben, Assistant United States Attorneys, files this response in opposition to the *pro se* motions of defendant Akhil Bansal and defendant Matthew Melao for the suppression of the electronic evidence obtained by law enforcement in this case. In their motions,¹ the defendants appear to be asking this Court to suppress or exclude from evidence virtually all of the electronic evidence seized, whether it was seized pursuant to search warrant or interception order. Their motions are based on fundamental misunderstandings of the law and should be denied. As explained more

¹ Bansal’s motion which is docketed at 309 appears to be, except for a different opening “statement” and “summary,” and the omission of a single paragraph at the conclusion, a literal copy of Melao’s motion which is docketed at 280. Bansal’s motion, which is docketed at 310 seeks to “amend/supplement” another motion to suppress, and consists of his attempt to inject the same ill-fated argument for suppression (that federal law enforcement agents are not allowed to apply for search warrants under 18 U.S.C. § 2703) which is briefly addressed herein.

fully below and in the government's responses to other motions in this case, the order authorizing the wiretap was properly issued, the emails at issue were electronic communications covered by the Wiretap Act, and even if there were a defect in the issuance or use of the wiretap in this case, suppression is not available as a remedy. Moreover, the email information which was acquired by search warrants was also lawfully obtained, and again, even if there were a defect in the issuance or use of any of the search warrants in this case, suppression is not available as a remedy. There is no basis for suppression of the electronic communications which the government intends to introduce at trial, nor is there any basis for ruling the evidence inadmissible.

I. INTRODUCTION

A. Factual Background

Defendants Akhil Bansal and Matthew Melao and fifteen of their co-defendants have been charged together in a 44-count indictment with conspiring to distribute and import controlled substances, engaging in a continuing criminal enterprise, conspiring to introduce into interstate commerce misbranded prescription drugs, money laundering and conspiring to commit money laundering.

During the lengthy investigation which led to the defendants' indictment, the government at different times sought and obtained search warrants to acquire stored electronic communications related to various defendants pursuant to 18 U.S.C. § 2703(a). This allowed the government to seize emails² stored – at specific points in time – on the servers used by the

² The term "email" refers to "the transfer of a message in electronic form from one computer user to another, usually over a network. The message will often travel through a series of computer systems until it reaches its final destination, where it can be stored for retrieval by its

defendants to send and receive emails. The search warrants did not allow the government real-time acquisition of the contents of electronic communications as they were being transmitted.

In January of 2005, pursuant to Section 2518 of Title 18 of the United States Code, the government applied to a United States District Court Judge sitting in the Eastern District of Pennsylvania (“the EDPA Judge”) for a order authorizing the interception of electronic communications for two email accounts registered to the defendant. The requested order permitted the government to “wiretap” the defendant’s email accounts, and obtain the contents of his emails prospectively. To secure the wiretap, the government was required to satisfy the substantial and demanding requirements of the Wiretap Act. See 18 U.S.C. §§ 2518(1)(b), 2518(1)(c), 2518(1)(e), 2518(3)(d), 2518(4)(a) & 2518(5). Based on the government’s satisfaction of the requirements, the EDPA judge authorized the wiretap.

Defendants Bansal and Maleo now seek to suppress, it appears, all of the electronic evidence obtained by the government pursuant to that wiretap and the search warrants.

B. The Statutory Scheme

Two different federal statutes -- Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the Wiretap Act), as amended, 18 U.S.C. § 2510 et seq., and the Stored Communications Act, 18 U.S.C. § 2701 et seq. -- govern access to electronic data and communications. Although the two statutory schemes overlap to some degree, there are differences between them.

The Wiretap Act was intended to address the significant potential for invasion of privacy

intended recipient” Geoff Ralston, et al., *Electronic Mail, in Encyclopedia of Computer Science*, 637, 637-38 (Anthony Ralston, et al., eds. 4th ed. 2001).

into the most sensitive areas of our lives as the result of growing eavesdropping technology and reliance on communications service providers. Congress was concerned that the “tremendous scientific and technological developments that have taken place in the last century have made possible today the widespread use and abuse of electronic surveillance techniques. As a result of these developments, privacy of communication is seriously jeopardized by these techniques of surveillance.” S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2154 (“S. Rep. No. 90-1097”). To ensure the privacy of communications sent using new communication technologies, such as email, Congress amended Title III in 1986 to extend the privacy protections of the Wiretap Act to electronic mail and other electronic communications. *See* Electronic Communications Privacy Act, Pub. L. 99-508, 100 Stat. 1858 (“ECPA”); *see also In re Pharmatrak*, 329 F.3d 9, 16 (1st Cir. 2003).

Not surprisingly, given its grave privacy concerns, the Wiretap Act “intercept” prohibition is quite broad. The Act makes it unlawful to intercept or to procure anyone else to intercept any oral, wire, or electronic communication. 18 U.S.C. § 2511(1)(a). The Act also makes it unlawful to use or disclose an illegally intercepted communication. 18 U.S.C. § 2511(1)(c), (d). The Wiretap Act also provides a series of interrelated definitions for “wire communication,” “electronic communication,” and “oral communication.”

The term “electronic communication” is defined as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by wire, radio, electromagnetic, photoelectronic or photooptical system.” 18 U.S.C. § 2510(12) (emphasis added). That definition covers communications such as electronic mail (“email”) and faxes. The definition of “electronic communication” has some express exclusions. It “does not include,” for

example, wire and oral communications (such as phone calls and in-person conversations), tone-only paging signals, tracking device signals, and "electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds." 18 U.S.C. § 2510(12). "Electronic communication" does not exclude generally communications in "electronic storage," as defined under the Wiretap Act. 18 U.S.C. §2510(17) (recodified as 18 U.S.C. §2510(18)). "Electronic storage" is "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" as well as the storage of such communication "by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

The Stored Communications Act makes it unlawful for any individual to access intentionally a facility through which electronic communication services are provided "without authorization," or to do so in excess of an authorization, if the individual thereby "obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system." 18 U.S.C. § 2701. The Stored Communications Act thus would cover, for example, a hacker who accesses or deletes stored emails. The Stored Communications Act provides lesser penalties for its violation than the Wiretap Act. Compare 18 U.S.C. § 2701(b) (Stored Communications Act) with 18 U.S.C. § 2511(4)(b) (Wiretap Act). The Stored Communications Act also excludes from its criminal sanctions any person operating or providing an electronic communications service, such as email accounts. 18 U.S.C. § 2701(c)(3).

Both the Wiretap Act and the Stored Communications Act establish the showings that law enforcement officers must make in order to acquire electronic communications. The Wiretap Act requires a more compelling showing. Compare 18 U.S.C. §§ 2516-2518 with 18 U.S.C. §

2703. To obtain access to electronically stored communications, the government can use a search warrant or proceed by subpoena, just as the government might with respect to similar information stored in paper rather than electronic form. To conduct a wiretap, in contrast, the government must complete a detailed wiretap application. The application must, among other things, detail the offense being investigated and include a complete statement concerning (1) whether or not other investigative techniques have been tried and (2) whether and why those other techniques are unlikely to succeed or appear too dangerous. 18 U.S.C. § 2518(1)(b), (c). The heightened showing imposed by the Wiretap Act³ reflects the perception that ongoing eavesdropping on conversations and communications as they occur is a graver intrusion on personal privacy than the one-time snapshot provided by searches of written or stored materials.

II. DISCUSSION

A. The EDPA Judge had Jurisdiction to Authorize the Wiretap and Suppression Would Not Be Appropriate Even If the EDPA Judge Did Not Have Jurisdiction.

Defendant Bansal's first argument in his *pro se* motion (Docket No. 308) appears to be the same argument advanced in the motion filed by his counsel when he was represented (Docket No. 220). The government has already responded to this argument, and incorporates herein its response to the motion by Bansal when he was represented. As explained therein, the EDPA Judge who entered the Wiretap Order had authority to do so, suppression is not available, and the

³ The protection of privacy under the Wiretap Act does not end with the issuance of the wiretap order. The operation of a wiretap is subject to judicial oversight. 18 U.S.C. § 2518(6). Further, upon the expiration of the order, the fruits of the wiretap are immediately sealed and carefully controlled. 18 U.S.C. § 2518(8). In addition, Congress put in place mechanisms to ensure that both the courts and Congress maintain oversight of interceptions by law enforcement. *See* 18 U.S.C. § 2519(2) & (3) (setting forth interception reporting requirements to the Administrative Office of the U.S. Courts and Congress).

motion must be denied.

B. The Affidavit in Support of the Wiretap Was Adequate and Suppression Would Not Be Appropriate Even If There Were Omissions

Defendant Bansal's next argument in his *pro se* motion (Docket No. 308) also appears to be the same argument advanced in the motion filed by his counsel when he was represented (Docket No. 220). The government has already responded to this argument, and incorporates herein its response to the motion by Bansal when he was represented. As explained therein, the order provided adequate information about the nature and location of the communications facility as to which authority to intercept was to be granted, in satisfaction of the statutory requirement set forth in 18 U.S.C. § 2518(4)(b). The order directed "MSN Hotmail, a communication provider as defined in Section 2510(15) of Title 18," to provide the information, facilities and technical assistance necessary to carry out the order. See Order of January 12, 2005, page 4.

Furthermore, there was no bad faith or intent to mislead on the part of the government in obtaining this order. The accompanying application stated that the target e-mail accounts were "operated by MSN Hotmail within the Northern District of California," see Application at page 2, and the affidavit identified the address of MSN Hotmail as "1065 LaAvenida, Bldg. 4, Mountain View, California, within the Northern District of California," and stated that the application was filed in the Eastern District of Pennsylvania because it was "one of the locations where the offense conduct has occurred," and that the interception would take place in Philadelphia. See Affidavit at paragraphs 7-9.

C. The Emails Could be Intercepted Pursuant to The Wiretap Act and Even If They Could Not, Suppression is Not An Available Remedy.

Defendant Bansal's next argument in his *pro se* brief seems to be that emails "are not

electronic communications” and therefore could not be “intercepted.” This argument appears to be the same argument advanced in the motion filed by his counsel when he was represented (Docket No. 220). The government has already responded to this argument, and incorporates herein its response to the motion by Bansal when he was represented. As explained therein, the emails were subject to “interception” pursuant to the Wiretap Act, and even if they were not, suppression is not an available “remedy.”

D. The Fact that MSN Hotmail Used Its Own Equipment Is Not a Violation of Any Statute, and Even if It Were, Suppression is Not Available.

Defendant Bansal’s next argument is one seemingly advanced by his co-defendant, Sanjeev Srivastav, in his “Omnibus” Pretrial Motions (Docket Nos. 213 & 298). The government hereby incorporates its response to those motions into this pleading. As explained therein, see Government’s Response to Defendant Srivastav’s Omnibus Pre-trial motion (Docket No. 213) and Supplemental Omnibus Pre-trial motion (Docket No. 298) at p. 19, n. 12, MSN Hotmail’s use of its own equipment to effectuate the Court’s Order does not provide the defendant with any grounds for suppression.

E. The Affidavit Sufficiently Sets Forth Why Normal Investigative Procedures Appeared Unlikely to Achieve the Goals of the Investigation.

The defendant complains that the government, when applying for the wiretap on his email accounts, failed to provide a sufficient factual predicate regarding normal investigative procedures. The defendant, however, has mischaracterized both the applicable law and the detailed information contained in the affidavit supporting the wiretap application.

Given the fact that a wiretap authorization is presumed to be proper, see United States v. Quintana, 70 F.3d 1167, 1169 (10th Cir. 1995), a defendant bears the burden of demonstrating

that contested wiretap evidence should be suppressed, including when his suppression claim rests upon the necessity requirement. See id.; cf. United States v. Acosta, 965 F.2d 1248, 1257 n.9 (3d Cir. 1992)(proponent of suppression motion generally has burden).

Title III requires the judge approving an application to find that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous." 18 U.S.C. § 2518(3)(c); see also § 2518(l)(c)(requiring affiants to provide such information). The Third Circuit repeatedly has explained that the requirement actually imposed by § 2518(3)(c) is not as onerous as the defendant suggests. For example, in United States v. Williams, 124 F.3d 411, 418 (3d Cir. 1997), the Third Circuit recently reaffirmed the following principles:

In Title III cases, courts have consistently held that 18 U.S.C. § 2518(3)(c) does not require the government to exhaust all other investigative procedures before resorting to electronic surveillance. . . . "The government need only lay a factual predicate' sufficient to inform the judge why other methods are not sufficient." Furthermore, in determining whether this requirement has been satisfied, a court "may properly take into account affirmations which are grounded in part upon the experience of specially trained agents . . . the government's showing is to be 'tested in a practical and common-sense fashion.'"(citations omitted).

See also United States v. McGlory, ,968 F.2d 309, 345 (3d Cir. 1992) (holding the same); United States v. Phillips, 959 F.2d 1187, 1189-1190 (3d Cir. 1992)(although defendant insisted that wiretap is valid only if other investigative methods have been exhausted or would be too dangerous or impractical, court declined to adopt such a strict interpretation); United States v. Armocida, 515 F.2d 29, 38 (3d Cir. 1975)(wiretap statute only requires existence of factual predicate regarding normal investigative procedures in affidavit for application).

Consistent with the pragmatic approach which courts employ when reviewing attacks

based upon § 2518(3)(c) , the Third Circuit has observed that "[i]nvestigators are not obliged to try all theoretically possible approaches." United States v. Vento, 533 F.2d 838, 849 (3d Cir. 1976). As long as the government avoids routinely employing electronic surveillance as the initial step in investigations, and fully explains why it is requesting authorization of electronic surveillance, "[i]t is sufficient that the government show that other techniques are impractical under the circumstances and that it would be unreasonable to require pursuit of those avenues of investigation." Id. Although a factual predicate consisting merely of "boiler plate" allegations unrelated to the circumstances of the case at issue will be insufficient, applications which "combine statements about general investigative experience in the type of crime and the particular facts of the case at hand" are satisfactory. Id. at 850 n. 19. Ultimately, "the statutory burden on the government is not great in showing compliance with § 2518(3)(c)." Armocida, 515 F.2d at 38; accord United States v. Oriakhi, 57 F.3d 1290, 1298 (4th Cir. 1994)(burden imposed by 2518(3)(c) is "not great;" courts should employ "practical and common-sense" review of government's factual predicate that avoids "hamper[ing] unduly the investigative powers of law enforcement agents"); United States v. Geller, 560 F.Supp. 1309, 1322-23 (E.D.Pa. 1983)(burden is "not great"); United States v. Baynes, 400 F.Supp. 285, 299 (E.D.Pa. 1975)(holding the same).

Electronic surveillance is appropriate where, as here, there was a strong probability of ongoing illegal activities, and the full extent of these crimes could not otherwise be probed satisfactorily. United States v. Vastola, 670 F. Supp. 1244, 1282-1283 (D.N.J. 1987); United States v. Armocida, 515 F.2d 29, 38 (3d Cir. 1975).

The affidavit submitted in support of the initial intercept, a copy of which is attached as

Exhibit 1, contained ten pages that outlined the affiant's position that the interception of electronic communications was the only available technique that had a reasonable likelihood of securing the evidence necessary to achieve the goals of the investigation, which included "the determination of the extent of the Bansals' drug importation and distribution network, including the identities of individuals who supply and purchase controlled substances and non-controlled pharmaceutical drugs unlawfully, the means of payment for these shipments, the laundering of proceeds derived from this unlawful activity, the location of criminal proceeds and assets, and to determine the methods of operation used by the participants in that network." See Affidavit at paragraphs 96-130.

The affiant described the investigative procedures that were unsuccessfully attempted, reasonably appeared unlikely to succeed if tried, or were tried with limited success, all in relation to the facts and circumstances and goals of the investigation. The following reasons were provided to show why physical surveillance was of limited usefulness without the real-time monitoring of the target e-mail accounts that electronic surveillance could provide:

1) because bulk shipments of the drugs originated outside the United States, it was not possible to know where and how the illegal shipments were entering to establish surveillance from their points of entry or from their multiple destinations within the United States; 2) the apparent use of commercial courier services also made it virtually impossible, without advance notice, to establish evidence of these bulk importations; 3) while physical surveillance had proven valuable in identifying some activities of targets and resulted in the seizures of a limited number of packages containing prescription drugs, it had not succeeded in gathering sufficient evidence of the full scope of criminal activity under investigation, and the elements of the violations; 4)

physical surveillance had failed to establish the identities of many of the conspirators; and 5) was not expected to enlarge upon available information and would most likely be noticed, causing the subjects to become more cautious in their illegal activities, to flee to avoid further investigation and prosecution, or to otherwise compromise the investigation.

The affiant also explained why subpoenaing persons believed to be involved in the conspiracy and their associates before a federal grand jury would not have been successful in achieving the stated goals of this investigation. First, if any of the principals of this conspiracy, their co-conspirators and other participants had been called to testify before the grand jury, they would most likely invoke their Fifth Amendment privilege not to testify, and seeking any kind of immunity for these persons would be unwise, because it could foreclose prosecution without ensuring truthful testimony. Second, the service of such grand jury subpoenas would only alert the recipients to the existence of the investigation, causing them to become more cautious, to encrypt all of their electronic correspondence, to flee, as the principal targets were foreign nationals with substantial ties – and assets – outside the United States, to destroy evidence, or to otherwise compromise the investigation.

As described in the affidavit, there was only one cooperating source with connections to the targets - defendant Richard Dabney, who identified codefendants Akhil Bansal and Atul Patil as the persons who paid him to mail packages. Dabney, because of his peripheral role, had virtually no knowledge of the scope of the enterprise, its activities, or its participants. Moreover, once Dabney told Bansal and Patil that some the packages had been seized by police and found to contain drugs, they ceased all contact with him.

Another potential cooperating witness, a pharmacist on federal probation in an unrelated

criminal case, was mentioned as a potential cooperator who could be possibly utilized in an attempt to purchase bulk quantities of controlled substances from the target subjects. The affidavit noted, however, that even if this witness was successful, as a purchaser whose only contact with the target subjects was likely to be through e-mail, the witness would not be privy to information that would achieve the goals of the investigation.

The affiant described the undercover activities conducted to date by a federal agent, which consisted of three undercover purchases of generic forms of controlled prescription drugs from one of the websites believed to be supplied by the target subjects. The website did not require a prescription and no doctor ever contacted the agent. Because all contact was through e-mail, the agent was unable to learn any useful information concerning the participants or their methods of operation. The purchases have served to show only the means by which the agents' undercover credit card accounts were charged for the drugs for their particular purchases, and to establish the nature of the drugs being sent to customers from that particular website.

The affiant also explained that interviews of the named interceptees would not achieve the goals of the investigation, because they would not produce information of the identities of all of the participants, would also produce a lot of false information and false leads, and more importantly, would alert the targets and subjects, compromising the investigation and resulting in the likely destruction or concealment of evidence and flight.

The search warrants that had been employed prior to the submission of the affidavit to date were described. One resulted in the recovery 119 packages, which were shipments made by Richard Dabney on behalf of Bansal and Patil. Another resulted in the recovery of nine UPS boxes and one box from the United States Postal Service (USPS) seized in connection with their

investigation into the activities of Armstrong Wholesale and target subjects David Armstrong and Elizabeth Armstrong. Through this search warrant, agents determined that nine of the ten boxes contained controlled substances. No locations associated with the Armstrongs were searched at the time so as not to alert them to the existence of the investigation.

The affidavit also described the execution of search warrant on the dedicated server that housed websites operated by Andrew Shackleton, who was charged in a separate indictment. Although the search yielded a considerable amount of information concerning Shackleton's activities, including stored e-mail messages that identified Brij Bansal and Akhil Bansal as one of Shackleton's suppliers, and some evidence of the wire transfer of funds from Shackleton to the Bansals' bank accounts in India in payment for the drugs, there was very little correspondence between the Bansals and Shackleton.

A search warrant served upon MSN Hotmail for subscriber information and e-mails stored within the e-mail accounts that were the subject of the wiretap application resulted in the acquisition of 2,731 stored e-mails, which demonstrated that Akhil and Brij Bansal were supplying controlled and non-controlled prescription drugs to customers in the United States and elsewhere. The e-mails discussed shipments of drugs to the United States and alluded to the Bansals' use of possibly corrupt Customs officials to ensure that their shipments passed undisturbed through Customs.

Five search warrants were also served upon companies that owned servers hosting websites and associated e-mail accounts. One of the servers contained the e-mail accounts associated with David and Elizabeth Armstrong (who were charged with their participation in the charged conspiracy in the Eastern District of New York). That search yielded a total of 2,118

messages contained in the two accounts. Some of the e-mails discussed specific shipments.

The other four search warrants involved four servers containing e-mail accounts pertaining to websites associated with Klaus Rieder and Corinna Mehrer (who were also charged with their participation in the charged conspiracy in the Eastern District of New York).

The affidavit explained that while valuable information was obtained through use of all of these search warrants, there was essential evidence that could not be obtained in this manner for the following reasons: 1) past e-mail messages which had been read and deleted were not available through such a search; 2) the search warrant on the target e-mail accounts appeared to have yielded only a small percentage of the e-mails that had been sent and received by these accounts by the time the warrants were served; 3) although the seized e-mails provided a far more detailed picture of the criminal conduct than had been available previously, they did not provide any information concerning when and where shipments entered the United States so that they could be intercepted and establish the nature and quantity of the drugs being shipped; 4) the seized e-mails did not usually identify – other than by first name and e-mail address – most of the individuals who corresponded with the Bansals about the offenses under investigation; and, finally, 5) the use of all of these search warrants did not, and, in all likelihood, would not, achieve the primary goals of the investigation, which, as noted above, were to determine the extent of the drug importation and distribution network, the identities of the individuals and businesses supplying the drugs, the methods by which the drugs are shipped into the United States, how they are stored, packaged, and distributed once they enter the United States, the identities of individuals within the United States who purchase the drugs in bulk for resale, and the flow of proceeds from these importations and distributions.

The affidavit also noted that a search of Akhil Bansal's apartment in Philadelphia, and any computer located there, might have yielded some previously received mail messages and attachments, such as spread sheets and invoices, but would not reflect the identities of those in the chain of distribution. Similar searches of the e-mail accounts, homes and computers of the other named interceptees would not have revealed the identities of all of the people and businesses who were sources and purchasers of the drugs.

For these reasons, the affiant stated that an ongoing electronic surveillance of the target email account accounts was the only means by which all of the information to achieve the goals of the investigation could be obtained. Furthermore, the affiant set forth his belief that search warrants executed on the targets' residences and computers would compromise the investigation by alerting the named interceptees, and others who have yet to be identified, to the existence of this investigation.

The affiant also described the pen register information had been used to date, which included pen registers on the target Hotmail accounts, on cellular phones used by Akhil Bansal and Atul Patil, and on hard-line telephones used by Akhil Bansal and Ashok Bhanushali. Additionally, In New York, pen registers had been obtained for cellular telephones subscribed to David and Elizabeth Armstrong. The affidavit acknowledged that the pen registers yielded limited useful information which strengthened the suspicion that the target subjects used the target e-mail accounts as their primary means of communication. The pen registers on the cellular telephones of David and Elizabeth Armstrong, however, showed minimal activity and further supported the conclusion that the members of this conspiracy used electronic mail as their primary form of communication. The affiant also pointed out that pen registers, even when

productive, do not record the identity of the parties to the conversation, cannot identify the nature or substance of the computer transmissions or differentiate between legitimate computer transmissions and transmissions related to criminal purposes. Telephone toll information was similarly limited, did not show local calls, and was generally available only on a monthly basis.

The affiant's recitation concerning the use of other investigative techniques was based on his training and experience, as well as that of his fellow agents, conversations with experienced prosecutors, and addressed the unique facts and circumstances of this investigation, and therefore satisfied the requirement set forth in Section 2518(3)(c).

This case is analogous to United States v. Armocida, 515 F.2d 29 (3d Cir. 1975), and other cases affirming the district court's necessity finding. In Armocida, the wiretap affidavit had revealed a history of physical surveillance, utilization of informants, undercover agents, and other wiretap interceptions. The affidavit explained, however, that the informant would not testify, surveillance was too easily noticeable and could jeopardize the investigation, and a search warrant was unlikely to reveal the identities of those believed involved in the narcotics conspiracy or the source of the narcotics. The Third Circuit held that this was sufficient to support the necessity finding made by the district court. Armocida, 515 F.2d at 38. Although the normal investigative techniques had identified one of the defendants as a "street-level" distributor, they had not been effective in achieving the objectives of the investigation, which was "to ascertain the scope of the alleged narcotics conspiracy and to identify the participants." Id. Thus, even though the government had "evidence sufficient to prosecute one of the conspirators, it is unrealistic to require the termination of an investigation before the entire scope of the narcotics distribution network is uncovered and the identity of its participants learned." Id.

The instrumentalities of Title III are properly employed when, as here, there is a strong probability of the existence of ongoing illegal activities, and the full extent of these crimes and conspiracies cannot otherwise be probed satisfactorily. See United States v. McGlory, 968 F.2d at 345 (wiretap necessary to discover content of conversations between conspirators); United States v. Adams, 759 F.2d at 1114 (despite successful undercover drug purchases, normal investigative methods would have risked discovery of investigation); United States v. Vento, 533 F.2d at 850 (wiretap was appropriate tool to discern full extent of conspiracy); United States v. Baynes, 400 F. Supp. 285, 298-300 (E.D.Pa. 1975).

Suppression of evidence is an extreme remedy. Accordingly, the Supreme Court ruled in Leon v. United States, 468 U.S. 897 (1984), that illegally seized evidence should not be suppressed if the investigating agents relied in "good faith" upon the authorization of a neutral and detached magistrate when obtaining the evidence. The Leon "good faith" doctrine applies to motions to suppress wiretap evidence. See United States v. Meling, 47 F.3d 1546, 1553 (9th Cir. 1995); United States v. Moore, 41 F.3d 370, 376-77 (8th Cir. 1994); United States v. Malekzadeh, 855 F.2d 1492, 1497 (11th Cir. 1988); United States v. Gotti, 42 F.Supp. 2d 252, 267 (S.D.N.Y. 1999). Therefore, even if this Court finds that the affidavit deficient, the evidence recovered as a result of the order authorizing the interception should not be suppressed if the agents relied upon the order in good faith.

F. The Delays in Sealing the Recordings Do Not Justify Suppression.

The defendant next argues that the electronic communications intercepted as a result of the Title III intercepts should be suppressed because the recordings were not sealed immediately after the final authorization order expired, as required by 18 U.S.C. § 2518(8)(a), which requires

that recordings of “the contents of any wire, oral, or electronic communication” be sealed “[i]mmediately upon the expiration of the period of the order, or extensions thereof . . .” under the direction of the judge issuing the order. Because the manner in which the recordings were sealed was consistent with Section 2518(8)(a) as interpreted by the Third Circuit, his claim should be denied.

The interceptions of the electronic communications at issue were conducted from January 12, 2005 to February 10, 2005, and from March 3, 2005 to April 1, 2005. The recordings obtained pursuant to the initial authorization were sealed on February 17, 2005; the recordings obtained pursuant to the first (and only) extension of that authorization were sealed on April 11, 2005.

One of the more recent and comprehensive discussions of the sealing requirement of 2518(8)(a) by the Third Circuit was set forth in United States v. Quintero, 38 F.3d 1317 (3d Cir. 1994). The defendants in Quintero challenged the district court's refusal to suppress certain telephone recordings obtained by a Title III wiretap, asserting that the tapes were not sealed immediately after the final authorization order expired, as required by statute, and that the government failed to offer a satisfactory explanation for the delay in sealing.

The electronic surveillance in question was conducted pursuant to three thirty-day authorizations: 1) the first authorization expired on August 30, 1991 (“August tapes”) - the tapes were sealed 11 days later, on September 10, 1991; 2) the authorization for the first extension expired on September 29, 1991 (“September tapes”) - the tapes were sealed 5 days later, on October 5, 1991 (the emergency judge); and 3) the authorization for the second and final extension expired on October 29, 1991 (“October tapes”) - the tapes were sealed 20 days later, on

November 18, 1991. Id. at 1321-22. The Third Circuit first determined that because the extensions were a continuation of the initial interception authorization, the tapes from the initial authorization and first extension did not have to be sealed until the termination of the entire wiretap on October 29, 1991. Because both were sealed before the wiretap terminated on October 29, 1991, the Third Circuit held that the district court properly admitted the tapes obtained by both authorizations. Id. at 1326.

The court of appeals held that the October tapes should have been suppressed because the government failed to supply a satisfactory explanation for the 20-day sealing delay, which the government conceded was not “as soon as administratively practical,” the interpretation of “immediately” adopted by the Third Circuit for the purposes of Section 2518(8)(a). Id. at 1330.

The Quintero court applied the test forth in United States v. Ojeda Rios, 495 U.S. 257, 260 (1990), in which the Supreme Court held that § 2518(8)(a) contains “an explicit exclusionary remedy for noncompliance with the sealing requirement,” and determined that, in the absence of a timely sealing, the government must “explain not only why a delay occurred but also why it is excusable.” Id. at 265. The Third Circuit noted that it had twice previously evaluated whether the government's delay in sealing tapes could be excused based on a “satisfactory explanation” provided by the government in United States v. Vastola, 989 F.2d 1318 (3d Cir.1993) (issue was whether the prosecutor's mistaken view of the law was objectively reasonable), and United States v. Carson, 969 F.2d 1480 (3d Cir.1992).

In Carson, the court of appeals held that there were two kinds of justifiable government delays under Section 2518: 1) “relatively short delays necessitated by the process required to comply with the provisions of the Act,” and 2) “longer delays attributable to non-administrative,

objectively reasonable causes like understandable mistakes of law and interference from unexpected, extrinsic events beyond the government's control.” Id. at 1326. See Carson, 969 F.2d at 1488. The Quintero court rejected the government’s explanation that a reasonable explanation for the 20-day delay was the trial schedules of the Assistant United States Attorneys involved in the case, concluding that “a prosecutor's routine duties, hectic as that routine may be, are not a satisfactory explanation for failing to comply with the immediacy requirement of § 2518(8)(a).” Id. at 1330.

1. The Recordings Obtained as a Result of the First Authorization Were Sealed As Soon as Administratively Practicable and Are Admissible.

The initial authorization ended on February 10, 2005; the recordings were sealed on February 17, 2005. The gap of 7 days between the expiration of the authorization and sealing of the recordings is not outside of the sealing requirement of Section 2518(8)(a) as interpreted by the Third Circuit. See United States v. Carson, 969 F.2d at 1487-88. In Carson, the Third Circuit has construed "immediately" in section 2518(8)(a) to mean that recordings must be sealed "as soon as administratively practical." 969 F.2d at 1487. In Carson, the Third Circuit held that sealing conducted after a delay of 6 days was "as soon as administratively practical" for the purposes of Section 2518(8)(a) and thus required no additional justification or explanation. 969 F.2d at 1498. The Carson court noted that the intervening weekend was a factor. Id. The panel in Carson also found that a 14-day sealing delay was not "immediate," but was excused by the prosecutor's reasonable mistake of law concerning the limits on (and consequences of) delay, based on the fact that Ojeda Rios had not yet been decided. Id. at 1492-93. The court of appeals also opined that a 10-day sealing delay would not often qualify as "as soon as administratively

practical." Id. at 1490. The district court below had simply assumed that a 10-day delay was not immediate and required an explanation. Id. at 1493. The Third Circuit remanded the case to the district court to decide this question. Id. at 1496. Under this standard, the 7-day delay in this case (which included one weekend) in sealing the recordings obtained by the initial authorization can reasonably be characterized as sealed "as soon as administratively practical," since it is only 1 day longer than the 6-day delay that was the subject of one of the holdings of Carson. See United States v. Quintero, 38 F.3d at 1329 (court declined to determine whether a 7-day delay would be acceptable, also noting that the length of the delay is a factor in considering whether the explanation for the delay is satisfactory).

2. The Recordings Made Pursuant to the First Authorization Are Admissible Because The Second Authorization Was an Extension of the First and the Recordings Made Pursuant to the First Authorization Were Sealed Before Expiration of the Second Authorization.

Section 2518(8)(a) of Title III does not require that the recordings to be sealed immediately after the expiration of each 30-day period; recordings from an original order need only be sealed upon the termination of the last extension of that order. 18 U.S.C. § 2518(8)(a). See United States v. Quintero, 38 F.3d at 1326; United States v. Carson, 969 F2d at 1487-88. The "second order need not be entered before the expiration of the first in order to qualify as an extension," provided the subject, location and criminal subject matter are the same, and "the new authorization was obtained as soon as administratively practical or any delay is satisfactorily explained." Id. at 1488. Delays in obtaining an extension can be justified by the administrative process of applying for an extension, and other events, including "understandable mistakes of law" and events beyond the government's control. Id. Gaps between orders may justifiably be

longer than delays in sealing because "more time is needed to secure an extension than to obtain the sealing order." Id. at 1489. The Third Circuit in Carson held that a gap of 17 days between the expiration of one authorization and the start of the next was "unduly long" absent extenuating circumstances. Id.

In the instant case, the first intercept order expired on February 10, 2005; the second order was issued on March 3, 2005. Even deducting at least one weekend, as explicitly permitted in Quintero, as well as one day for President's Day, results in a 17-day delay.⁴ Thus, under Carson, the government would arguably be required to provide a reasonable explanation for the delay, which could include the requirement to seek review and approval from Justice officials in Washington or the emergence of probable cause to continue an interception only near the end of the initial 30-day period. See id. at 1490 & n.4. To the extent that it is necessary, the government is prepared to present evidence concerning the reasons for the delay. See United States v. Plescia, 48 F.3d 1452, 1463 (7th Cir. 1995)(court held that government's explanation for 20-day delay between periods of interception was reasonable "as necessary to draft the Title III surveillance request affidavit and to get the request processed by the federal bureaucracy").

3. The Eleven-Day Delay in Sealing in the Recordings Obtained as a Result of the First Extension of the Initial Authorization Was Reasonable; Therefore the Recordings Are Admissible.

The second sealing order was not entered until April 11, 2005; the authorization expired on April 1, 2005. Because the 11-day delay is closer to the 14-day delay in Carson that required an explanation, as opposed to the 6-day period that did not, the government is prepared, if

⁴ The government does not concede that the two additional weekends between February 10 and March 3 should not be deducted, a question left open in Quintero, 38 F.3d at 1327 n.7.

necessary, to present testimony pertaining to a reasonable explanation for the delay.⁵

G. The Defendant Has Not Shown that There Are False Statements in the Sealing Application and Orders

The defendant alleges that the sealing application and order contained a typographical error concerning the notification requirement - Section 2518(d) instead of 2518(8)(d) - and then states that the error was unlawful. This argument does not merit further discussion. Similarly, the allegedly false statement by the AUSA in the sealing application that 20 individuals were

⁵ The majority of the e-mails (and attachments) that were obtained by the Title III interception were also obtained via search warrants that were obtained after the initial interception and during and after the first extension and from the defendants' computers that were recovered during the arrests of April 19, 2005. Even if the Court declines to accept the government's explanation for the delay in sealing the recordings obtained during the first extension as reasonable, the e-mails obtained by search warrants that were based, in part, on information obtained as a result of the Title III interception, would not necessarily be suppressed under Section 2518(8)(a). The suppression provision of Section 2518(8)(a) refers specifically to "the use or disclosure of the contents of any wire, oral, or electronic communication or evidence derived therefrom under subsection (3) of section 2517." Section 2517 defines the uses to which law enforcement officers can use the contents of a Title III interception or evidence derived therefrom as follows: 1) "disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure; 2) "use such contents to the extent such use is appropriate to the proper performance of his official duties;" or 3) "disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof." 18 U.S.C. §§ 2518(8)(a)(1) - (3). Because Section 2518(8)(a) refers specifically to Section 2517(3), and not to 2517 generally, the statutory suppression remedy under Section 2518(8)(a) appears to be limited to the use of recordings or transcripts at trial. To hold otherwise would effectively bar the disclosure and use in the course of an investigation as authorized under 2517(1) and (2), which are expressly excluded from the reach of 2518(8)(a). The Second Circuit, the only federal appeals court to address this question, has adopted this position. United States v. Donlan, 825 F.2d 653, 655-57 (2d Cir 1987) (sealing delay does not require the exclusion at trial of evidence, not mentioned in intercepted conversations, obtained when officers make a stop and search on the basis of such conversations). The Third Circuit has acknowledged but declined to rule on this issue in two later cases. See United States v. Carson, 969 F.2d 1480, 1500 (3d Cir. 1992); United States v. Vastola, 915 F.2d 865, 876 n.19 (3d Cir. 1990).

charged was correct - 17 in the instant case and 3 in the case of U.S. v. Andrew Shackleton, et al., Cr. No. 05-194, which charged the defendants with conspiring with Ahkil Bansal and the other supplier defendants.

H. The Defendant Has Not Set Forth Any Other Legitimate Basis For Challenging the Admissibility Suppression of the Electronic Evidence

The defendant presents a rambling discussion of various aspects of electronic surveillance on pages 20 - 35 of his motion. As discussed in this and prior motion responses, most of the emails and attachments that will be presented in this case were obtained by search warrants, Title III interceptions, and from the defendant's computers. The only portion of the motion from pages 20-35 that merits any response is the defendant's allegations of false statements in the affidavit. Most of the examples given by the defendant reflect, at best, inconsistencies. Any allegations of false statements must be evaluated in light of Franks v. Delaware, 438 U.S. 154, 155-56 (1978), in which the Supreme Court established a two-step procedure to be followed when a defendant makes a claim that a search warrant affidavit contains a false statement or material omission. First, the defendant must make a substantial preliminary showing that the affidavit contains an intentional or reckless falsehood or omission.⁶ Id. A defendant must come forward with "allegations of deliberate falsehood or of reckless disregard for the truth, and those allegations must be accompanied by an offer of proof." Id. at 171. See United States v. Jackson, 65 F.3d 631, 635 (7th Cir 1995) (Franks applies to wiretap affidavits), vacated in part on other

⁶ If the defendant does so, the court must hold a hearing. At such hearing, the defendant bears the burden of proving, by a preponderance of the evidence, that the allegations regarding the false statements are true. Id. at 156. Under Franks, however, even if the Court finds that the affiant made an intentional or reckless omission, suppression is not appropriate unless the defendant also proves that the omitted information, if included, would have made a difference to the probable cause determination. Id. at 171-72.

grounds on rehearing, 74 F.3d 751 (7th Cir 1996). The defendant has failed to do so, therefore his allegations should be rejected.

I. The E-mails Which the Government Will Introduce As Evidence Will Be Authenticated.

In “Part IV(D)” of his *pro se* motion, defendant Bansal argues that the “emails presented by government as ‘evidence’ are inadmissible in the Court,” and then, invoking various principles governing the authentication and admission of evidence, seems to set forth his belief that the government will be unable to prove that he sent the emails which were obtained from his computer and his email accounts. In this regard, he is sadly mistaken, as the government will be able to authenticate the electronic evidence, and will seek its admission through a number of accepted bases.⁷

The admission of computer records generally raises two distinct issues. First, the government must establish the authenticity of all computer records by providing "evidence sufficient to support a finding that the matter in question is what its proponent claims." Fed. R. Evid. 901(a). Second, if the computer records are computer-stored records that contain human statements, the government must show that those human statements are not inadmissible hearsay.

⁷ Defendant Bansal also appears to assert that the fact that in its compliance with the Wiretap Order, MSN Hotmail made a mirror or “clone” account of the defendant’s account for the government somehow undermines the authenticity of what the government acquired. The government’s evidence will include testimony about the process for “cloning” the defendant’s account which will prove the authenticity of the electronic evidence. This evidence will show that the “cloning” process produced a perfect copy of the e-mail messages. Under Rule 1003, a duplicate is admissible to the same extent as the original, unless there is a genuine question about the authenticity of the original. Fed. R. Evid. 1003. The copy can be authenticated by showing that the process used to produce it produces an accurate result. Fed. R. Evid. 901(b)(10). Thus, by showing that the cloning process produced an accurate copy, the government will authenticate the clone or duplicate.

At the trial in this case, the government will establish both the authenticity and admissibility of the electronic evidence which it seeks to introduce.

1. Authentication

Before a party may move for admission of a computer record or any evidence, the proponent must show that it is authentic. That is, the party must offer evidence "sufficient to support a finding that the [computer record or other evidence] in question is what its proponent claims." Fed. R. Evid. 901(a). "All that is required is a foundation from which the fact finder could legitimately infer that the evidence is what its proponent claims it to be." In re: Japanese Electronic Products, 723 F.2d 238, 285 (3d Cir. 1983), *rev'd on other grounds*, Matsushita Electric Industrial Co., Ltd., v. Zenith Radio Corporation, 475 U.S. 574 (1986). This is a prima facie showing only and the evidence from which this finding is made must itself be admissible (in contrast to rulings under Fed. R. Evid. 104(a)). Once a prima facie showing has been made, if authenticity is disputed, the dispute is to be resolved by the jury. Id. The standard for authenticating computer records is the same for authenticating other records. The degree of authentication does not vary simply because a record happens to be (or has been at one point) in electronic form. See United States v. Vela, 673 F.2d 86, 90 (5th Cir. 1982); United States v. DeGeorgia, 420 F.2d 889, 893 n.11 (9th Cir. 1969). But see United States v. Scholle, 553 F.2d 1109, 1125 (8th Cir. 1977) (stating in dicta that "the complex nature of computer storage calls for a more comprehensive foundation"). For example, witnesses who testify to the authenticity of computer records need not have special qualifications. The witness does not need to have programmed the computer himself, or even need to understand the maintenance and technical operation of the computer. See United States v. Salgado, 250 F.3d 438, 453 (6th Cir. 2001);

United States v. Moore, 923 F.2d 910, 915 (1st Cir. 1991) (citing cases). Instead, the witness simply must have first-hand knowledge of the relevant facts to which she testifies. See generally United States v. Whitaker, 127 F.3d 595, 601 (7th Cir. 1997) (FBI agent who was present when the defendant's computer was seized can authenticate seized files); United States v. Miller, 771 F.2d 1219, 1237 (9th Cir. 1985) (telephone company billing supervisor can authenticate phone company records); Moore, 923 F.2d at 915 (head of bank's consumer loan department can authenticate computerized loan data).

In this case, defendant Bansal seems to be challenging the authenticity of computer-stored records by questioning the identity of their author. The evidence in this case, however, will include overwhelming circumstantial evidence of defendant Bansal's authorship of his emails. For example, with respect to the MSN Hotmail accounts, the government's evidence will include, among other things, the facts that: both accounts were established by the defendant, who gave his address as the address which will be shown to be the defendant's; the defendant was listed as the user of one of the accounts and that his father and co-defendant, Brij Bansal, was listed as user for the other account; extra storage on the accounts was paid for by the defendant with a Visa credit card; the same Visa credit card which was used to pay the accounts was taken from defendant at the time of his arrest; the defendant consistently signed the emails with his name; the defendant admitted to law enforcement agents after his arrest that he used both of the hotmail accounts to run his illegal drug distribution operation; the defendant repeatedly provided the hotmail account as his email address; and files taken from the defendant's computer, compact disks and jump drives (all recovered from the defendant's home) have e-mails and spreadsheets that match ones obtained by the government through the wiretap or search warrants. Such

evidence will certainly exceed the standard prima facie showing and will provide ample authentication of the electronic evidence. See United States v. Siddiqui, 235 F.3d 1318, 1322-23 (11th Cir. 2000) (e-mail messages were properly authenticated where messages included defendant's e-mail address, defendant's nickname, and where defendant followed up messages with phone calls); see also United States v. Simpson, 152 F.3d 1241, 1250 (10th Cir. 1998)(upholding admission of printout of an Internet chat conversation between undercover agent and defendant when circumstantial evidence showed that name used in chat room was alias of the defendant); United States v. Tank, 200 F.3d 627, 630-31 (9th Cir. 2000).

2. Admissibility

When a computer record contains the assertions of a person, whether or not processed by a computer, and is offered to prove the truth of the matter asserted, the record may contain hearsay.⁸ Of course, admissions by a party-opponent and statements made by co-conspirators of a party and during the course and in furtherance of the conspiracy are defined as “not hearsay” by the Federal Rules of Evidence. Fed. R. Evid. 801(d)(2). Furthermore, well-established exceptions to the rule against hearsay existence, including the exception which permits the

⁸ When a computer record contains only computer-generated data untouched by human hands, however, the record cannot contain hearsay. Fed. R. Evid. 801(c) requires that hearsay be a “statement.” Rule 801(a) defines a “statement” as an oral or written assertion of a person or nonverbal conduct of a person, if it is intended by the person as an assertion. To the extent that the records offered are generated solely by a computer (such as computer logs), they are not statements because they are not made by a person. In such cases, the government must establish the authenticity of the record, but does not need to establish that a hearsay exception applies for the records to be admissible in court. See State v. Armstead, 432 So.2d 837, 840 (La. 1983). See also People v. Holowko, 486 N.E.2d 877, 878-79 (Ill. 1985) (automated trap and trace records); United States v. Duncan, 30 M.J. 1284, 1287-89 (N-M.C.M.R. 1990) (computerized records of ATM transactions); 2 J. Strong, McCormick on Evidence § 294, at 286 (4th ed.1992); Richard O. Lempert & Stephen A. Saltzburg, A Modern Approach to Evidence 370 (2d ed. 1983).

admission of business records, Fed. R. Evid. 803(6) and other statements which have circumstantial guarantees of trustworthiness equivalent to the hearsay exceptions, Fed. R. Evid. 807, are set forth in the Federal Rules of Evidence. In this case, the government will meet the legal requirements for admissibility of all of the electronic evidence it will introduce.

J. The Volume of Emails Is Not a Grounds for Excluding Them.

In his final argument, defendant Bansal contends that “most of” the “thousands of emails and hundreds of spreadsheets” which the government “wishes to present” are “irrelevant in context of the case,” and that the “sheer number of irrelevant emails” will “create a risk of unfair prejudice, confusion of issues, misleading the jury, or cause undue delay, waste of time, or needless presentation of cumulative evidence,” and moves the Court to exclude “these emails.” All of the electronic evidence that the government intends to present was sent in furtherance of the conspiracies charged in the indictment. While a substantial amount of electronic evidence will certainly be moved in by the government at trial, not all of it will be displayed to the jury and much of it will be presented in summary fashion. The defendant is obviously free to oppose the admission of any specified communication; however, his motion as stated should be denied.

K. The Government’s Use of A Search Warrant to Obtain Emails Was Lawful and Appropriate, and Even if There Were Errors, Suppression is Not Available.

Defendant Melao, in his *pro se* suppression motion (Docket No. 280) makes a number of assertions that appear to be trying to advance arguments similar to those advanced by defendant Bansal, and which are responded to above. Defendant advances some additional arguments,

however, none of which presents any valid basis for suppression.⁹ Defendant Bansal argues, somewhat opaquely, that the government's use of a search warrant under 18 U.S.C. §2703(a) to obtain the email messages and associated records stored in an email account was "unlawful as per [the Stored Communications Act]." Melao *pro se* Mot. at 7. This claim is baseless, and should be rejected.

At the outset, defendant Melao is correct that e-mail received by a recipient's service provider but not yet accessed by the recipient is in "electronic storage." See Orin S. Kerr, A User's Guide to the Stored Communications Act – and a Legislator's Guide to Fixing It, 72 Geo. Wash. L. Rev. 1208, 1217 (2004) ("email is in 'electronic storage' awaiting [the user's] retrieval of the message" from the service provider). Further, defendant Melao correctly notes that law enforcement must, as a general matter, obtain a search warrant in order to compel an Internet service provider to disclose such electronic communications in "electronic storage." See 18 U.S.C. §2703(a).

The defendant does not argue, however, that the government failed to adhere to the

⁹ Melao's arguments that federal law enforcement agents are legally distinct from, and not included within, the "government entity" referenced in the statute as able to require disclosure from an electronic communication service, see Melao *pro se* Br. at pp. c-1 to c-7, and that an order to compel an electronic communication service provider to "disclose" information is somehow legally distinct from legal authority to "acquire or seize" the information, see Melao *pro se* Br. at pp. 8-9, do not warrant discussion. 18 U.S.C. § 2703. Needless to say, "government entities" can act only through their agents and representatives, and Congress clearly contemplated that federal law enforcement agents would be among the persons allowed to apply for search warrants. See 18 U.S.C. § 2703(g), providing that the "officer" need not be present for the service or execution of the search warrant. Similarly, in the context of search warrants for the contents of electronic communications, "disclosure" of the "contents" has no separable meaning from a seizure of the electronic data which comprises the communications. The defendant's requests for suppression and "punishment" of the agents must be rejected.

dictates of section 2703(a); indeed, the government's use of a valid search warrant forecloses any such claim. Instead, the defendant asserts that the government also received other stored messages not in "electronic storage,"¹⁰ and that this receipt somehow violated the Act. He is incorrect, and the motion to suppress should be denied.

Most obviously, defendant Melao fails to note that 18 U.S.C. §2703 provides a comprehensive mechanism for obtaining any customer record from an Internet service provider by means of a search warrant. Some content records – for example, unopened email – can only be obtained via warrant. See 18 U.S.C. §2703(a). There is only one other category of communications content protected by the Stored Communications Act: communications held by a provider in its capacity as a "remote computing service." See 18 U.S.C. §2703(b). This category comprises any message stored by a service provider after the user has accessed it and retrieved a copy, such as "opened" email.¹¹ Critically, Defendant's argument ignores the fact that such "opened" messages may also be obtained by means of a warrant. See 18 U.S.C. §2703(b)(1)(A); Kerr at 1220.

To the extent that defendant Melao argues that non-content records (such as the log files requested in Paragraph 4 of the Attachment to the warrant) may not be obtained with a warrant, he is again mistaken. Section 2703(c)(1) explicitly permits the government to compel "a record

¹⁰ We note that defendant Melao fails to specify which messages received by the government were allegedly not in "electronic storage." As explained below, however, this defect is immaterial because the defendant's underlying legal claim is wrong.

¹¹ "[W]hen an e-mail customer leaves a copy of an already-accessed e-mail stored on a server, that copy is no longer [in 'electronic storage']; rather, it is just in remote storage like any other file held by [a 'remote computing service']." Kerr at 1217.

or other information” other than contents by a wide variety of means, including a search warrant. See 18 U.S.C. § 2703(c)(1)(A).¹²

Moreover, assuming that any violation of the Stored Electronic Communications Act was committed, there is no suppression remedy for such a violation. See 18 U.S.C. §§ 2707 & 2708; United States v. Smith, 15 F.3d 1051, 1056 (9th Cir. 1998) (“the Stored Communications Act [chap. 121] expressly rules out exclusion as a remedy”); United States v. Charles, 1998 WL 204696 at *21, No. Crim. 97-10107-PBS (D. Mass. Jan. 13, 1998) (“ECPA provides only a civil remedy for a violation of § 2703”), aff’d, 213 F.3d 10 (1st Cir. 2000); United States v. Reyes, 922 F. Supp. 818, 837-38 (S.D.N.Y. 1996) (“Exclusion of the evidence is not an available remedy for this violation of the ECPA The remedy for violation of Title II of the ECPA [*i.e.*, chap. 121] lies in a civil action.”). For these reasons, defendant Melao’s motion to suppress should be denied.

L. Neither Defendant Has Not Set Forth Any Other Basis For Suppression of the E-Mails Obtained by Search Warrant.

The defendants make a number of additional allegations in an attempt to suppress the emails obtained by search warrants. See Bansal motion #309 at pages 15-37; Melao motion # 280 at pages c-1 to c-7, 15-37. The allegations are identical; both recite a number of definitions in support of his arguments that the affiants were not authorized to apply or execute the warrants. Melao motion at c-1 to c-7; Bansal Motion to Amend (Docket No. 310). These arguments are

¹² Defendant’s corollary argument – that the government violated 18 U.S.C. § 2701 by improperly acquiring the contents of communications – ignores the exception in Section 2701(c)(3), which ratifies the use of the various compulsory mechanisms set out in Section 2703.

without merit and should be denied.

They also allege that the warrants did not contain sufficient probable cause, without identifying any specific warrant or affidavit. These arguments, to the extent that they merit a response, are without merit and should be rejected. The affidavits, which are attached hereto with the warrants as Exhibit 2, set forth sufficient facts which established, to the magistrate judge's satisfaction, probable cause to believe that the defendants' email accounts contained evidence of various violations of the federal law.

A magistrate judge may find probable cause when, viewing the totality of the circumstances, "there is a fair probability that contraband or evidence of a crime will be found in a particular place." Illinois v. Gates, 462 U.S. 213, 238 (1983). This Court must uphold the finding if the affidavit on which it was based provided a substantial basis for finding probable cause. See Id. at 236; United States v. Jones, 994 F.2d 1051, 1054-55 (3d Cir. 1993); United States v. Conley, 4 F.3d 1200, 1205 (3d Cir. 1993). The Court need not determine whether probable cause actually existed, but only whether there was "a 'substantial basis' for finding probable cause." Jones, 994 F.2d at 1054; Conley, 4 F.3d at 1055, 1057.

Because of the preference for searches conducted pursuant to warrants, challenges to such searches generally should be rejected in cases in which the issue of whether probable cause exists is close. United States v. Whitner, 219 F.3d 289, 299 (3d Cir. 2000). The Fourth Amendment does not require direct evidence linking the crime to the location to be searched to support the issuance a search warrant. Probable cause can be established by circumstantial evidence that establishes a fair probability that evidence of a crime or contraband will be found at the location

to be searched. United States v. Burton, 288 F.3d 91, 103 (3d Cir. 2000); United States v. Jones, 994 F.2d at 1056. A court "is entitled to draw reasonable inferences about where evidence is likely to be kept, based on the nature of the evidence and the type of offense." United States v. Whitner, 219 F.3d 289, 296 (3d Cir. 2000) (quoting United States v. Caicedo, 85 F.3d 1184, 1192 (6th Cir.1996)).

In this case, the affidavits provided ample basis for the reasonable inference that the defendants were using their email accounts to conduct and further their illegal drug importation and distribution scheme. The affidavits, read in their entirety, clearly provided a substantial basis for the magistrates to conclude that there was a fair probability that evidence of involvement in the illegal scheme then under investigation was likely to be found in the defendants' email accounts. This information, particularly in light of the nature and scope of the scheme at issue and the logical inferences from the rest of the affidavit, provided ample probable cause to justify a warrant to search the defendants' email accounts.

However, even if this Court were to find that there was not sufficient probable cause to support the issuance of the warrants to search the defendants' email accounts, the evidence that was recovered pursuant to the warrants should not be suppressed, because the agents relied on the warrants in good faith. Evidence seized pursuant to a warrant should not be suppressed "when an officer executes a search in objectively reasonable reliance on a warrant's authority." United States v. Williams, 3 F.3d 69, 74 (3d Cir. 1993). The purpose of the exclusionary rule is to deter unlawful police conduct. United States v. Leon, 468 U.S. 897, 906 (1984). Thus, if a law enforcement officer has obtained a warrant and executed it in good faith, "there is no police illegality and thus nothing to deter." Id. at 921. The fact that an officer executes a search

pursuant to a warrant is prima facie evidence of good faith. United States v. Hodge, 246 F.3d 301, 308 (3d Cir. 2001).

The mere existence of a warrant typically suffices to prove that an officer conducted a search in good faith and justifies application of the good faith exception. Leon, 468 U.S. at 922; Williams, 3 F.3d at 74. Of course, there are a few situations in which an officer's reliance on a warrant is not reasonable and will not trigger the exception. These occur when: (1) the judge issued the warrant in reliance on a deliberately or recklessly false affidavit; (2) the judge abandoned his judicial role and failed to perform his neutral and detached function; (3) the warrant was based on an affidavit "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable;" or (4) the warrant was so facially deficient that it failed to particularize the place to be searched or the things to be seized. Williams, 3 F.3d at 74 n. 4 (citations omitted).

Plainly, none of these exceptions apply here. The defendants cannot credibly claim that the good faith exception should not be applied because the warrants were based on an affidavit so lacking in probable cause that no reasonable officer could rely on any one of them as the basis for a search warrant. To determine whether the good faith exception applies in the face of this challenge, the Court must determine "whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization." United States v. Loy, 191 F.3d 360, 367 (3d Cir. 1999) (citations omitted). See also United States v. \$ 92,422.57, 307 F.3d 137, 145-46 (3d Cir. 2002). Based on the record and the affidavits in this case, the agents' reliance on the warrants was objectively reasonable, and the evidence obtained pursuant to these warrants should not be suppressed.

Furthermore, the affidavits sufficiently identified the suspected violations and the items to be seized. The execution of the warrants was done in conformity with the law. The defendants have not set forth any facts that indicate otherwise.

Many of the arguments alleged by the defendants in this section are alleged and addressed elsewhere. The nature of most of the defendants' allegations is illustrated by their contention that the bad faith of DEA Special Agent Eric Russ was exemplified by his deliberate submission of eight search warrants to magistrate judges on Fridays, knowing that he could get the warrants more easily that way. Bansal motion at 28. Because these allegations are without any factual or legal basis, they should be rejected.

WHEREFORE, the United States respectfully requests that this Court enter an order denying the *pro se* motions of defendant Akhil Bansal at Docket Nos. 308, 309 and 310 and defendant Matthew Melao at Docket No. 280 for the suppression of the electronic evidence obtained by law enforcement in this case.

Respectfully submitted,

PATRICK L. MEEHAN
United States Attorney

FRANK R. COSTELLO, JR.
BEA L. WITZLEBEN
Assistant United States Attorneys

CERTIFICATE OF SERVICE

I certify that on this the day of 2006, I caused this pleading to be electronically filed ,
and caused a copy of this pleading to be served upon the following by first class mail:

Akhil Bansal, *Pro Se*

USM# 59593-066

Federal Detention Center

700 Arch Street

Philadelphia, PA 19106

Richard Harris, Esquire

El-Shabazz & Harris LLC

100 S. Broad Street, Suite 1525

Philadelphia, PA 19110

Standby Counsel for Akhil Bansal

J. Michael Farrell, Esquire

718 Arch Street, Suite 402-S

Philadelphia, PA 19106

Counsel for Sanjeev Anand Srivastav

Steven G. Laver, Esquire

1515 Market Street, Suite 1915

Philadelphia, PA 19102

Counsel for Frederick Mullinix

a/k/a “Tom Peters”

Matthew Melao, *Pro Se*

USM# 33230-177

Federal Detention Center

700 Arch Street Philadelphia, PA 19106

Henry S. Hilles, III, Esquire

509 Swede Street

Norristown, PA 19401

Standby Counsel

for Matthew Joseph Melao

Anne M. Dixon, Esquire

Stephen R. LaCheen & Associates

1429 Walnut Street, Suite 1301

Philadelphia, PA 19102

Counsel for Kelly Ann Couchman

a/k/a “Kelly Mullinix”

Robert J. O’Shea, Jr., Esquire

1818 Market Street, Suite 3520

Philadelphia, PA 19103

Counsel for Christopher Geoff Laine

FRANK R. COSTELLO, JR.

BEA L. WITZLEBEN

Assistant United States Attorneys